Estudios Políticos 60

ARTÍCULO

La inviolabilidad de las comunicaciones desde la protección de datos personales

The inviolability of communications from the protection of personal data

Gabriel Espinoza Ibarra*

Recibido: 4 de mayo, 2023. Aceptado: 14 de junio, 2023.

Resumen La hipótesis del estudio es que la protección de datos personales - de forma genérica - tiene un rasero de protección que no pone énfasis en las comunicaciones privadas como un dato personal de especial relevancia. Por lo tanto, resulta mucho más sencillo para las autoridades del sector público el transgredir las comunicaciones basados en argumentos sustentados en defensa de la seguridad u orden públicos. Es decir, las numerosas excepciones en el derecho a la protección de datos personales habilita a las autoridades del sector público para realizar esta clase de intervenciones.

Palabras claves: México, inviolabilidad de comunicaciones, protección de datos personales, Pegasus, espionaje.

Summary The hypothesis underlying our study is that the protection of personal data - in a generic sense - has a protection standard that does not emphasize private communications as a personal data of special relevance. Therefore, it is much easier for public sector authorities to transgress communications based on arguments supported by defense of security or public order. In other words, the numerous exceptions in the right to the protection of personal data enable public sector authorities to carry out this type of intervention.

Keywords: Mexico, inviolability of communications, protection of personal data, Pegasus, espionage.

* Licenciado en Ciencias Políticas y Administración Pública. Líneas de investigación: acceso a la información, protección de datos, rendición de cuentas.

Introducción.

En México, las comunicaciones privadas están protegidas desde el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Se dice así en razón que este precepto reconoce dos derechos. El derecho a la protección de datos personales y el relativo a la inviolabilidad de las comunicaciones. Ambos se reconocen para todas las personas en el territorio nacional.

De este modo, las comunicaciones se interrelacionan con numerosos derechos — a manera de ejemplo: la libertad de expresión, de asociación, privacidad e intimidad—. Por ende, es esencial que se cuenten con vías jurídicas para su protección por vías judiciales y no jurisdiccionales.

Así, la finalidad del estudio que nos ocupa versa en comparar los paralelismos entre la regulación de la inviolabilidad de las comunicaciones y la protección de datos personales. Este estudio, además, se estima que resulta relevante para efectos de nuevas líneas de investigación en razón que no se advierte que se haya efectuado previamente un comparativo de las comunicaciones privadas a la luz de las disposiciones en la materia de protección de datos personales.

Así, la hipótesis en la que descansa nuestro estudio radica en que la protección de datos personales - de forma genérica - tiene un rasero de protección que no pone énfasis en las comunicaciones privadas como un dato personal de especial relevancia. Por lo tanto, resulta mucho más sencillo para las autoridades del sector público el transgredir las comunicaciones basados en argumentos sustentados en defensa de la seguridad u orden públicos. Es decir, las numerosas excepciones en el derecho a la protección de datos personales habilita a las autoridades del sector público para realizar esta clase de intervenciones con un menor nivel de escrutinio.

Asimismo, la problemática detectada radica en analizar las comunicaciones privadas a la luz del derecho a la protección de datos personales pues se advierte que un solo fenómeno se regula de manera distinta por parte de esos dos derechos; cuestión que se evidencia a través de dos casos concretos. Por un lado, el expediente Pegasus derivado de un presunto caso de espionaje a cargo de la entonces Fiscalía General de la República[1] y por otra parte el espionaje del defensor de derechos humanos Raymundo Ramos por parte de la Secretaría de la Defensa Nacional.[2]

Por ende, se estima que el estudio resulta ser pertinente en razón que, en ambos casos, el actual presidente de la república, Andrés Manuel López Obrador, ha afirmado desde la conferencia matutina, que él mismo dirige, que se realizan actividades de intervención de comunicaciones por parte de las fuerzas armadas justificados en una suerte de actividades de seguridad a las que catalogo como actividades de inteligencia.

Es por esta razón que el tema que abordamos resulta importante, pues a partir de estos sucesos resulta posible el tratar de volver lícitas actividades de espionaje por parte de las autoridades en contra de los particulares; lo anterior, amparados en presuntos razonamientos de seguridad nacional.

[1] El caso es de amplio conocimiento y fue documentado por los medios de comunicación. Solo para dar cuenta de uno de ellos, véase: Pegasus: el programa que espía a políticos y gobiernos. *La Vanguardia*, 09 de mayo, 2022. https://www.lavanguardia.com/vida/junior-report/20220509/8248278/pegasus-espionaje-politicos-gobiernos.html

[2] *El Ejército mexicano espió con Pegasus al activista Raymundo Ramos para interferir en una investigación sobre ejecuciones extrajudiciales*, *El País*, 07 de marzo, 2023. https://elpais.com/mexico/2023-03-07/el-ejercito-mexicano-espio-con-pegasus-al-activista-raymundo-ramos-para-interferir-en-una-investigacion-sobre-ejecuciones-extrajudiciales.html

Por lo que hace al alcance de la investigación, en este estudio se pretende describir las disposiciones jurídicas vigentes en relación con el derecho a la inviolabilidad de comunicaciones y la protección de datos personales. Así, a partir de dos casos de estudio, esto es, Pegasus y el defensor de derechos humanos Raymundo Ramos, se delimita el objeto de estudio en cuestión, pues resultan ser fenómenos que se encuentran ampliamente documentados y resulta posible extraer conclusiones sobre el tratamiento que ha tenido la autoridad en lo relativo a las comunicaciones privadas.

En consecuencia, esta investigación tiene como objetivo principal el identificar el presunto trato diferenciado desde dos derechos distintitos para un solo bien jurídico, esto es, las comunicaciones privadas. Adicionalmente, de forma secundaria, se pretende evidenciar que este trato diferenciado permite a las autoridades el transgredir las comunicaciones privadas a partir de la óptica de las presuntas actividades de inteligencia que se sustentan en el marco jurídico de la protección de datos personales.

Un objetivo adicional consiste en documentar cuál ha sido el resultado de las indagatorias por parte del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI o Instituto en adelante) a raíz de los casos de espionaje antes mencionados.

I. De los conceptos en torno a las comunicaciones privadas.

En este apartado haremos referencia a las disposiciones conceptuales y jurídicas que corresponden a dos derechos humanos contenidos reconocidos expresamente en la Constitución Política de los Estados Unidos Mexicanos: la protección de datos personales y la inviolabilidad de las comunicaciones privadas. Ambas referencias se estiman relevantes con la finalidad de dar mayor claridad al tema en estudio.

I.I. Las disposiciones en torno a la inviolabilidad de comunicaciones

De esta forma, es relevante mencionar que la inviolabilidad de las comunicaciones es un derecho humano, el cual se encuentra presente en el texto de la Constitución Política de los Estados Unidos Mexicanos en su artículo 16 en sus párrafos primero, doceavo y décimo tercero. De estas disposiciones se obtiene el siguiente contenido:

- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.
- Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

- Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

En esta misma línea, el artículo 12 de la Declaración Universal de Derechos Humanos, adoptada en 1948, indica que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Adicionalmente, el artículo 11.2 de la Convención Americana sobre Derechos Humanos, dispone que:

> Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

Asimismo, es relevante dar cuenta de los criterios judiciales en la materia. Es así que, con base en el Amparo Directo en Revisión 1621/2010 de fecha 15 de junio de 2011, dio cuenta en torno a este derecho que "*lo que se encuentra prohibido por el artículo 16 constitucional es la interceptación o el conocimiento antijurídico de una comunicación ajena, por lo que la violación se consuma en el momento en que se escucha, se graba, se almacena, se lee o se registra –sin el consentimiento de los interlocutores– una comunicación ajena, con independencia de que, con posterioridad, se difunda el contenido de la conversación interceptada*."

En este sentido, es de destacarse que la inviolabilidad de las comunicaciones se encuentra protegidas con independencia del medio en el cual se desarrollan; tan es así que, para tales efectos dictó la tesis cuya denominación es: DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. Su ámbito de protección se extiende a teléfonos o aparatos de comunicación abandonados o respecto de los cuales no se tenga conocimiento de quién es su titular, por lo que para acceder a su información debe solicitarse la autorización de un Juzgador Federal.

De este modo, el criterio de referencia en su parte conducente, consignó que, la violación del derecho referido se consuma en el momento en que se escucha, graba, almacena, lee o registra -sin el consentimiento de los interlocutores- una comunicación ajena, con independencia de que con posterioridad se difunda el contenido de la conversación interceptada. En estas condiciones, para que sea constitucional la intervención de cualquier comunicación privada, en términos del referido artículo, deberá existir, indefectiblemente, control judicial previo por parte de un juzgador integrante del Poder Judicial de la Federación. Consecuentemente, al poseer el derecho a la inviolabilidad de las comunicaciones privadas, autonomía propia y al configurar una garantía formal que protege las comunicaciones con independencia de su contenido.

En este sentido, la Suprema Corte de Justicia de la Nación ha tenido oportunidad de pronunciarse sobre el carácter autónomo del derecho a la inviolabilidad de las comunicaciones

respecto de otros derechos, a través de la Tesis aislada 1a. CLIII/2011 denominada "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD". Sobre este aspecto, la Corte precisó que pese a ser una manifestación más de aquellos derechos que preservan al individuo de un ámbito de actuación libre de injerencias de terceros –como sucede con el derecho a la intimidad, a la inviolabilidad del domicilio o la protección de datos personales–, el derecho a la inviolabilidad de las comunicaciones privadas posee una autonomía propia reconocida por la Constitución.

Asimismo, la intervención de comunicaciones privadas tiene una configuración especial que limita al máximo la posibilidad de injerencias arbitrarias en la privacidad de los habitantes del país. Debe tenerse presente que intervenir comunicaciones privadas sin la autorización legal se configura como delito, de conformidad con el propio artículo 16 de la propia Ley Fundamental (Cienfuegos Salgado, 2012).

Para que la autoridad judicial conceda o niegue una solicitud de intervención de comunicaciones privadas, debe constatar dos aspectos: a) La existencia de indicios suficientes para suponer que la persona investigada es miembro de la delincuencia organizada, y b) Que la intervención es el medio adecuado para recabar información que sirvan para investigar a los miembros de la delincuencia organizada. Cabe recordar que, en ningún caso, el Juez podrá autorizar intervenciones de las comunicaciones privadas cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral, y administrativo, ni en el caso de las comunicaciones del detenido con su defensor (Cienfuegos Salgado, 2012, 164).

Dicha intervención, solamente es facultad del Ministerio público de la Federación; es decir, no lo puede realizar ninguna otra autoridad. Por lo tanto, es posible afirmar que existe una transgresión respecto de la expectativa razonable de la privacidad que se espera en una conversación entre ambas partes.

Finalmente, es necesario precisar que la violación a este derecho acontece en el momento en que se escucha, graba, almacena, lee o se registra – sin el consentimiento de los interlocutores – una comunicación ajena, por lo que la reserva de las comunicaciones se impone sólo frente a terceros; es decir, que no existe violación a ese derecho fundamental cuando alguno de los comunicantes autorice su intervención, con independencia de la posible configuración de la violación al derecho a la intimidad de conformidad con los Amparos directos en revisión 975/2018 y 1621/2010.

Adicionalmente, es necesario hacer referencia al contenido de la Ley Federal contra Delincuencia Organizada, la cual establece en sus artículos 16 y 17 que faculta al Ministerio Público a requerir la intervención de comunicaciones; a este respecto, cuando se considere necesaria la intervención de comunicaciones privadas conforme a las siguientes directrices:

- El Fiscal General de la República o los servidores públicos en quienes se delegue la facultad podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.
- La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo.

- La solicitud de intervención de comunicaciones privadas deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos y, en su caso, la denominación de la empresa concesionaria del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público de la Federación acredite nuevos elementos que así lo justifiquen

I.II El derecho a la protección de datos personales

Al respecto, a partir de los años setenta, se acuña el término sobre la "autodeterminación informativa" con base en el derecho general de la personalidad de la Ley Fundamental de Bonn, para referirse al derecho de los individuos a controlar su información en general. Posteriormente, en 1983 el Tribunal Constitucional Federal Alemán le da un contenido específico a este derecho señalando que los individuos podían disponer respecto al uso de sus datos personales, así como las condiciones para su revelación, otorgando a la autodeterminación informativa o libertad informática el carácter de derecho fundamental (Pascual Huerta, 2013).

Por otra parte, siguiendo a Marcela Basterra (Basterra, 2008:16-19), se menciona que este derecho – es decir, el de habeas data - consiste en *la posibilidad que tiene el titular de un dato personal de controlar quiénes serán destinatarios de dicha información y qué uso se dará a la misma*. De esta forma, este derecho tiene por objeto el:

> "(...) impedir que en bancos o registros se recopile información respecto de la persona titular del derecho que interpone la acción, cuando información esté referida a aspectos de su personalidad que se encuentren directamente vinculados con su intimidad, (...)Se trata particularmente de información relativa a la filiación política, ideas religiosas, militancia gremial, desempeño laboral, participación académica, etc."

Por lo tanto, se obtiene que la mencionada determinación personal que ejerce activamente el sujeto sobre sus datos rebasa la postura pasiva en determinación de no intromisión de su privacidad.

La protección de datos personales, por tanto, implica que toda persona tiene derecho a controlar sus datos personales, es decir, a decidir quién los recopila, cómo se utilizan, con qué fines, con quiénes se comparten y durante cuánto tiempo se mantienen almacenados.

Ahora bien, en el ámbito del derecho mexicano, el habeas data se encuentra reconocido como el derecho a la protección de datos personales. Así, de conformidad con lo dispuesto en artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, se desprende que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley.

Del mismo, modo se preé que la legislación secundaria establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Tomando la definición de datos personales establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados se obtiene que dato personal se define como cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información de conformidad con lo establecido en la fracción IX del artículo 3 de este instrumento normativo.

Consecuentemente, podemos decir que los datos personales se definen como cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo concerniente a una persona física identificada o identificable. Estos datos pueden incluir, por ejemplo, el nombre, la dirección, la fecha de nacimiento, la información de contacto, el estado civil, la ocupación, la fotografía, el número de identificación oficial, el número de seguridad social, entre otros

En este sentido, con base en estas definiciones, tenemos que la protección de datos personales establece límites del control del conjunto de información personal que hace a un individuo identificado o identificable.

Adicionalmente, tomando como base el Diccionario de Transparencia el dato es un sinónimo de información o unidad de conocimiento, y su vinculación con una persona física. El conector entre ellos implica descubrir la identidad de la persona a través de cualquier información que la identifica o que, bajo criterios de razonabilidad, la haga identificable, esto es, que la particularice y distinga frente a las demás. Esta relación puede manifestarse de manera directa, como en el caso de los datos de identificación o las imágenes o, de manera indirecta, a través del cruce o combinación de datos pertenecientes a categorías diversas que permiten identificar al individuo (Cejudo, 2019).

Al respecto, el Grupo de Trabajo del Artículo 29 ha sistematizado el debate a través de la descomposición del concepto de datos personales en cuatro categorías de análisis: (1) toda información; (2) sobre; (3) una persona (física); (4) identificada o identificable.

La segunda categoría de análisis a la que hace referencia el Dictamen 4/2007 de ese Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales, el cual se refiere al vínculo de la información con la persona. En algunos casos esta relación es evidente, pues hace una referencia directa. No obstante, en otros, alude a un objeto o registro y solamente a través de información adicional se identifica al individuo.

Así, sobre el segundo supuesto, es decir, la información que hace identificable a una persona, se tiene que estas relaciones que no resultan evidentes por sí mismas; tan es así como puede derivar de la homonimia, la geolocalización de las personas si es que, posiblemente, podrían hacer identificable a una persona.

Asimismo, para la jurista Solange Maqueo (Maqueo, 2019, pp. 260.) la protección de datos personales constituye un derecho que coadyuva a garantizar que el ámbito privado de las personas esté exento o inmune de injerencias abusivas o arbitrarias por parte de terceros (sean del sector público o privado). Por ello, establece las condiciones bajo las cuales el tratamiento de datos personales puede considerarse legítimo (lo que incluye cada una de las etapas que

constituyen el proceso al que son sometidos los datos) y dota de potestades específicas a los individuos para que estén en posibilidad de mantener un cierto poder de control y disposición sobre su información.

Estas dos últimas características del derecho a la protección de datos personales son, precisamente, las que han permitido su evolución de manera particularizada frente a otros derechos humanos, entre los que sin duda destaca, dada la estrecha relación que guardan entre ellos, el derecho a la vida privada y, con ello, la privacidad misma.

II. Las comunicaciones privadas desde el derecho a la protección de datos personales

Como hemos mencionado previamente, en los artículos 6 y 16 de nuestra Constitución, se prevé que la información que se refiere al ámbito privado de las personas, así como los datos personales, debe estar protegida en los términos y con las excepciones a los principios de tratamiento de datos que por razones de orden público fije la ley, por lo que toda persona tiene derecho a la protección de sus datos personales.

Asimismo, se reitera que la definición de datos personales prevista en la legislación secundaria se define como información confidencial a aquella sobre los datos personales concernientes a una persona física identificada o identificable de conformidad con el artículo 113, fracción I de la Ley Federal de Transparencia y Acceso a la información

De esta manera, se estima que la relación entre la protección de datos personales y la inviolabilidad de las comunicaciones son dos derechos fundamentales que están relacionados entre sí, pero que no son idénticos.

Como hemos visto hasta este punto, la inviolabilidad de las comunicaciones se refiere al derecho de las personas a que sus comunicaciones, ya sea por teléfono, correo electrónico u otros medios, sean privadas y no puedan ser interceptadas o espiadas sin que medie una orden judicial.

Por su parte, la protección de datos personales se refiere al derecho de las personas a controlar el uso que se da a su información personal, incluyendo datos como el nombre, dirección, número de teléfono, correo electrónico, entre otros.

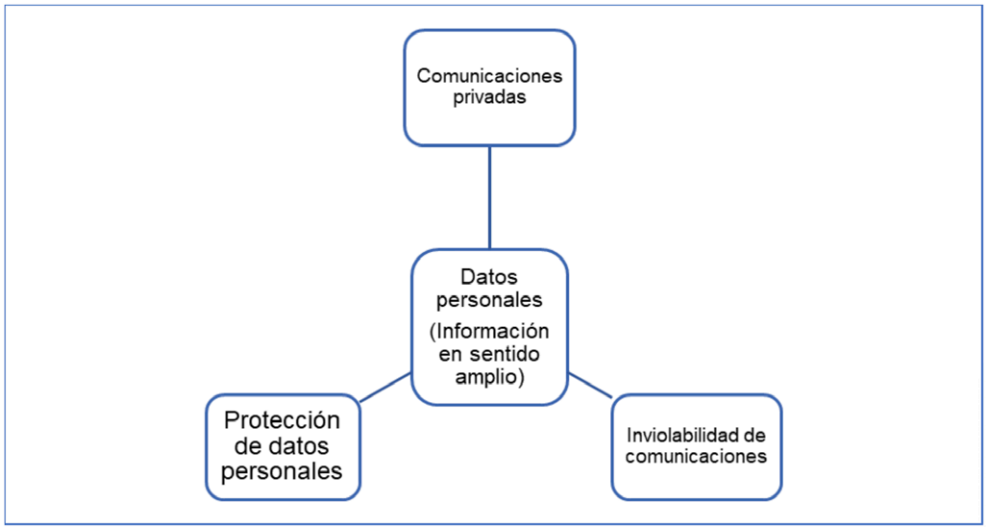
En consecuencia, como se ha dicho, toda vez que la protección de datos personales es la tutela respecto de la información personal, este ámbito de tutela se extiende, a manera de ejemplo, sobre correos electrónicos y mensajes de texto, al ser datos que se vinculan a una persona, se consideran como datos personales.

Bajo esa premisa, en el presente trabajo sostenemos que las comunicaciones son un dato personal y, por tanto, objeto de tutela de las disposiciones en materia de protección de datos personales.

Cuestión que es necesario se matizar, pues ello no implica que se excluya la observancia de las disposiciones sobre la inviolabilidad de comunicaciones privadas, sino el reconocimiento de las mismas dentro del ámbito de la regulación de datos personales y por ende, que se robustece el ámbito de tutela.

Consecuentemente, en caso de una transgresión de las comunicaciones privadas, se estima que de forma simultánea se estaría violando el derecho a la inviolabilidad de las comunicaciones y la protección de datos personales.

Por ende, se ilustra la concatenación de estos derechos conforme a la propuesta en el presente estudio:



Fuente: Elaboración propia.

Sobre este último aspecto es donde se centra nuestro objeto de estudio: la tutela de las comunicaciones privadas desde el derecho a la protección de datos personales. Estos derechos, además a través de dos casos de estudio: el espionaje de Pegasus efectuado desde la Fiscalía General de la República y la intromisión en las comunicaciones respecto de un defensor de derechos humanos por parte de las fuerzas armadas.

III. Procedimientos en materia de protección de datos personales

Recordemos que el derecho a la protección de datos personales contenido en el artículo 16 de la Constitución prevé que toda persona tiene este derecho, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

De este modo, toda vez que el presente caso versa respecto de tratamiento de datos personales en el sector público, resulta aplicable a lo dispuesto en artículo 1 de la Ley General de Datos el cual establece que son sujetos obligados por esa Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Por ende, a continuación, abordaremos dos figuras dispuestas en el marco jurídico de protección de datos personales. Por un lado, lo relativo al procedimiento de verificación y sanciones y, adicionalmente, las excepciones al consentimiento en esta materia. Tales elementos resultan indispensables para contar con mayor evidencia normativa que apunta a la forma en la que se

tratan las comunicaciones privadas a través de estas disposiciones. De la misma forma, en lo relativo al contraste entre ambos derechos.

Así, hasta este punto es posible verificar que, efectivamente existen mayores supuestos que permiten exceptuar el consentimiento del titular de los datos personales frente a la inviolabilidad de comunicaciones. Es decir, se cumple el objetivo toral, al evidenciar que el marco jurídico en materia de protección de datos faculta a las autoridades a acceder a datos personales, en este caso comunicaciones privadas.

Asimismo, queda claro que para acceder a las comunicaciones privadas no resulta necesario cumplir con requisitos elementales, como es el consentimiento de la o el titular y la orden judicial al tratar con información sensible como son las comunicaciones privadas.

III.I. Sobre el procedimiento de verificación y sanciones en materia de protección de datos personales.

Ahora bien, por lo que hace en estricto sentido al procedimiento previsto en la Ley General de Datos,[3] se desprenden toralmente las consideraciones siguientes:

Además de las facultades que el INAI detenta conforme al acceso a la información, tiene competencia para conocer, sustanciar y resolver los procedimientos de verificación;

El Instituto y los Organismos garantes, en el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los Organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

El procedimiento de verificación iniciará bajo dos supuestos

- De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o
- Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.
- El procedimiento de verificación concluirá con la resolución que emita el Instituto o los Organismos garantes, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.

Ahora bien, por lo que hace a las causas de sanción en materia de protección de datos personales se prevé en el citado instrumento normativo en sus artículos 163 y 165. Por lo cual, se establece que serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

- Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;
- Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se

[3] Conforme a lo establecido en los artículos 89 fracción VI, 146, 147, 149 y 150 de la Ley General en la materia.

trate; III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

- Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;
- No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de sus elementos;
- Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
- Incumplir el deber de confidencialidad
- No establecer las medidas de seguridad en
- Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad
- Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;
- Obstruir los actos de verificación de la autoridad;
- Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley (fuentes de acceso público)
- No acatar las resoluciones emitidas por el Instituto y los Organismos garantes
- Omitir la entrega del informe anual y demás informes o bien, entregar el mismo de manera extemporánea.

III.II. Excepciones al tratamiento de datos personales

Por lo que hace a las excepciones en el tratamiento de datos personales recordemos que desde la Constitución se establece que son excepciones:

- Razones de seguridad nacional.
- Disposiciones de orden público.
- Seguridad y salud públicas.
- Protección de los derechos de terceros.

Por su parte, la Ley General de Datos establece dos supuestos donde no es necesario requerir el permiso (consentimiento) de las personas titulares: esto es, a través de la excepción al consentimiento y por lo que se refiere a la transferencia de datos personales.

Por lo que hace a la excepción al consentimiento, prevista en el artículo 22 de este ordenamiento, el responsable no estará obligado a recabarlo del titular para el tratamiento de sus datos personales en los siguientes casos:

- Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;
- Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
- Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
- Cuando los datos personales figuren en fuentes de acceso público;

Asimismo, para efectos del artículo 70 de la Ley General de Datos, la autoridad podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:

- Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;
- Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
- Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;
- Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;
- Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;
- Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales; y
- Cuando la transferencia sea necesaria por razones de seguridad nacional.

IV. Sobre los casos de espionaje en concreto

A continuación, en el presente apartado abordaremos el espionaje efectuado a través del software Pegasus y en contra del defensor de derechos humanos Raymundo Ramos. Al respecto, se estima que tales casos resultan ser pertinentes en razón que a partir de la transgresión cometida contra las personas que fueron vulneradas en sus comunicaciones resulta posible advertir cuál fue la respuesta de las autoridades involucradas en las denuncias y la manera en la cual se aplicó el marco jurídico en cada uno de ellos.

IV.I. El caso Pegasus: software de espionaje telefónico

El caso de espionaje del software Pegasus en México dio cuenta del software de espionaje denominado como Pegasus, desarrollado por la empresa israelí NSO Group, el cual fue empleado en México para espiar a periodistas, activistas de derechos humanos y personas de la sociedad civil.[4]

Se tiene la estimación que más de quince mil personas fueron infectadas, además de 25 periodistas entre los cuales se encuentran: Carmen Aristegui, Jenaro Villamil, Marcela Turati, Alejandro Caballero, Álvaro Delgado, Rafael Rodríguez Castañeda, Jorge Carrasco, Ignacio Rodríguez Reyna, Arturo Rodríguez García, y Alejandra Xanice.[5]

A este respecto, conforme a lo descrito por el informático Fran Brizzolis, la operación del programa en cuestión opera de la siguiente forma (Brizzolis, 2019):

- El software es un spyware de "intercepción legal" para gobiernos y se infiltra en los teléfonos inteligentes y otros aparatos para monitorear cualquier detalle de la vida diaria de una persona por medio de su celular, ya sea a través de llamadas, mensajes de texto, correos electrónicos, contraseñas, contactos y calendarios.
- La compañía que fabrica el programa es la empresa israelí NSO Group, y exclusivamente lo vende a los gobiernos con la condición de que solo sea utilizado para combatir a terroristas o grupos criminales y cárteles de drogas.
- Pegasus es capaz de interceptar llamadas telefónicas, mensajes de texto y iMessages, recibir vídeo en directo de aplicaciones como FaceTime y Skype, tener acceso a correos electrónicos con todo y archivos adjuntos, activar cámaras y micrófonos de forma remota, así como vaciar toda la información contenida en el dispositivo.

Ahora bien, de acuerdo con la Red de defensa de derechos digitales (R3Dmx) en México, al menos tres dependencias han gastado casi 80 millones de dólares en estos programas de espionaje desde 2011, según el reporte del New York Times: la entonces Procuraduría General de la República (PGR), el Centro de Investigación y Seguridad Nacional (CISEN) y la Secretaría de la Defensa Nacional.

En este sentido, resulta importante hacer mención al contrato CISEN/33701/002/16, con el cual se habría comprado el malware Pegasus a la empresa Proyectos y Diseños VME por un monto de 203 millones de pesos. El contrato fue celebrado el 31 de mayo de 2016 y firmado por Eugenio Imaz, entonces director del CISEN.

En junio de 2017, medios de comunicación dieron a conocer la existencia de un contrato celebrado el 29 de octubre de 2014 entre la Procuraduría General de la República y Grupo Tech Bull, por un monto de 32 millones de dólares.

Por su parte, la SEDENA suscribió entre 2015 y 2018, 23 contratos con empresas como Proyectos y Diseños VME, KBH Track y Air Cap. Estas compañías han sido identificadas como

[4] El caso es de amplio conocimiento y fue documentado por los medios de comunicación. Solo para dar cuenta de uno de ellos, véase: Pegasus: el programa que espía a políticos y gobiernos, *La Vanguardia*, 09 de mayo de 2022. https://www.lavanguardia.com/vida/junior-report/20220509/8248278/pegasus-espionaje-politicos-gobiernos.html

[5] Así logró el software Pegasus espiar a 25 periodistas mexicanos, *Forbes* México, julio 2021, visible en: https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/

parte del entramado que ha celebrado contratos de Pegasus con la PGR y el CISEN, y que ha transferido dinero a la empresa israelí NSO Group.

Conforme será expuesto en un apartado posterior, este caso de espionaje telefónico llegó a ser investigado por parte del INAI a través del procedimiento de verificación antes analizado.

IV.II. Raymundo Ramos: el espionaje en contra de defensores de derechos humanos

Siete años después del contrato celebrado por parte de la entonces Procuraduría General de la República y un cambio de partido en el gobierno, se develó que producto del hackeo a los equipos informáticos de la Secretaría de la Defensa Nacional, las fuerzas armadas instruyeron a que se espiara al defensor de derechos humanos.

Esta investigación periodística llevada a cabo por parte Animal Político, Aristegui Noticias y Proceso expone una tarjeta informativa secreta de inteligencia militar.

En este documento, se busca vincular a Raymundo Ramos como integrante del Cártel del Noreste, sin ofrecer prueba alguna. El documento también aconseja al Secretario de la Defensa Nacional, Luis Crescencio Sandoval, presentar la información a la Policía Ministerial Militar de forma confidencial para las indagatorias del caso, sin que se agregue a la carpeta de investigación.[6] Esto demuestra que la intención del espionaje fue interferir ilegalmente en las investigaciones sobre los abusos cometidos en Nuevo Laredo por parte de las fuerzas armadas.

Así, las organizaciones de la sociedad civil manifestaron la ausencia de facultades legales por parte de las Fuerzas Armadas para intervenir comunicaciones, asimismo, enfatizaron que dicha intervención carece de autorización judicial.

Adicionalmente, destaca que el documento en el cual se consigna dichas actividades de espionaje fue realizado por parte de la Subjefatura de Inteligencia del Estado Mayor de la Defensa Nacional; por conducto del Centro Militar de Inteligencia. Con ello, se advierte con claridad que el Estado Mexicano no ha cesado las actividades de espionaje en contra de personas que no se relacionan con actividades de la defensa o seguridad nacional, ni tampoco por lo que hace al crimen organizado.

Es decir, la documentación nos permite vislumbrar que existe un aparato de inteligencia que sigue empleando software malicioso para intervenir equipos de periodistas y de defensores de derechos humanos. El agravante radica en que existe evidencia que la Secretaría de la Defensa Nacional ejerce estas funciones fuera del marco normativo.

Ahora bien, no pasa desapercibido que el Gobierno Federal publicó un pronunciamiento respecto del alcance de las acciones de inteligencia orientadas a la detección de riesgos para la seguridad nacional, de este boletín se destacan los elementos siguientes:

Según lo sostenido por parte del gobierno federal, la inteligencia es el conocimiento obtenido a partir de la recolección, procesamiento, diseminación y explotación de información para la toma de decisiones en materia de seguridad nacional, y el ciclo de inteligencia es el proceso que orienta las acciones de recolección y procesamiento de información con el propósito de

[6] Dicho documento puede consultarse en el siguiente vínculo electrónico: https://r3d.mx/wp-content/uploads/Tarjeta-Informativa-Raymundo-Ramos-Testada-scaled.jpg

integrarlas en productos de inteligencia para la toma de decisiones de con conformidad con el artículo 29 de la Ley de Seguridad Nacional

De acuerdo con el Gobierno Federal, las instancias de Seguridad Nacional, entre ellas la Secretaría de la Defensa Nacional, de manera conjunta con otras dependencias, trabajan en recolección, procesamiento, diseminación y explotación de la información, que comparten con otras autoridades en materia de seguridad pública, de conformidad con lo referido por el Gobierno Federal con base en los artículos 5, fracciones III, V y XI, 29, 30, 31, 33, 34 y 35 de la Ley de Seguridad Nacional y 100 de la Ley de la Guardia Nacional.

Tales procedimientos, según sostiene la autoridad, únicamente se realizan con el fin de coadyuvar a la procuración de justicia; sin embargo, han existido casos en que, de la información recabada por este tipo de actividades, algunas personas se han visto relacionadas con organizaciones delictivas.

De acuerdo con el comunicado, no se consideran oficiales algunos documentos que diversos medios de comunicación han dado a conocer, relacionándolos con el ciberataque sufrido a los servidores de la SEDENA. Que dichos documentos no están signados, firmados, ni avalados por alguna autoridad competente. Por tal razón, dichas publicaciones carecen de validez legal.

Todo el esfuerzo de inteligencia del Estado mexicano se dirige a combatir a la delincuencia organizada y narcotráfico, por lo que no se ha detenido a ningún actor político, social, persona perteneciente a una organización de derechos humanos, activista u otra persona que no esté relacionada con las organizaciones de la delincuencia organizada.

Bajo esta tesitura, a partir del pronunciamiento por parte del Gobierno Federal permite advertir un par de líneas que no son del todo congruentes entre sí, pues si bien se invocan facultades en materia del combate a la delincuencia organizada, no se configura ninguna atribución que de manera específica faculte a las fuerzas del orden público para intervenir, expresamente un derecho que es inviolable a nivel constitucional.

Por el contrario, se evidencia que, en efecto, la protección de datos personales por la vía de la seguridad nacional le permite a estas instituciones el ampararse para efectos de realizar intervenciones sobre comunicaciones en el combate del crimen organizado.

Finalmente, queda claro que no existe un reconocimiento respecto del uso o no del software o el método por el cual se interviene a estos presuntos grupos del crimen organizado sino que se limita a desvirtuar los documentos que derivan del hackeo a los sistemas informáticos de la SEDENA.

IV. III. El expediente sobre el caso Pegasus ante el INAI

En noviembre de 2018, ese Instituto comenzó con una investigación de oficio para efecto de determinar si la entonces Procuraduría General de la República (PGR) incumplió con la normativa en materia de protección de datos personales.

De este modo, se originó el expediente de verificación INAI.3S.07.01-007/2018 en términos de los parámetros del procedimiento de verificación antes descrito. Específicamente en lo relativo en los considerandos tercero, cuarto y quinto de la resolución contenidos en las páginas 200 a 274 de la misma y del boletín emitido por parte de ese Instituto es posible obtener los siguientes elementos:

- Se determinó que la entonces Procuraduría General de la República (PGR) incumplió con el deber de seguridad y el principio de responsabilidad, previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Que la PGR sólo notificó a al Instituto la existencia del contrato suscrito en 2014 para la adquisición del software; sin embargo, posterior al dictado del procedimiento de verificación dio cuenta de la existencia dos contratos más celebrados en 2016 y 2017, para actualizar la licencia de uso del sistema, obstruyendo con dicha conducta los actos de verificación del Instituto.
- Derivado del procedimiento en cuestión el INAI determinó instruir a la Fiscalía General de la República el que instrumentara las siguientes medidas:
- Acreditar que el software denominado fue desinstalado de los equipos de la Fiscalía así como de la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas de la Agencia de Investigación Criminal.
- Precisar las políticas, que dan cuenta de la desinstalación del software; así como, acreditar fehacientemente que no es factible instalar nuevamente el software adquirido en algún equipo en posesión de la ahora Fiscalía General.
- Que la Fiscalía General de la República publique en versión pública de los contratos celebrados en 2016 y 2017, para la actualización de la licencia de uso del software.

Así, del procedimiento de verificación al que le recayó el expediente mencionado, se advierte que se tuvo por transgredido el principio de responsabilidad y el deber de seguridad, en razón que la autoridad no contaba con un sistema de gestión y con un documento de seguridad, respecto del sistema para la realización de actividades sustantivas.

Asimismo, no se acreditó el borrado del sistema y la generación por parte de dicho sistema de bases en las que se resguardan dichos datos y al carecer de una bitácora de uso del sistema.

Como consecuencia de ella, el INAI determinó el dar vista a la Auditoría Superior de la Federación, a efecto que verifique los bienes adquiridos y los servicios contratados por la entonces Procuraduría General de la República que impliquen alguna suerte de irregularidad.

Asimismo, se presentó una denuncia ante la propia Fiscalía General de la República por considerar que presumiblemente se configura una conducta antijurídica sobre el ejercicio ilícito de servicio público. Lo anterior, en razón que la PGR informó que no contaba con bitácoras de uso o registros, bases de datos y aplicaciones que dieran cuenta de la utilización del sistema adquirido por la entonces Procuraduría General de la República, ni constancia de su instalación o desinstalación de los equipos en su posesión; a pesar de que con base en los contratos de adquisición y licenciamiento que debieron existir.

Con todo, debemos de precisar que de la resolución contenida en el expediente INAI.3S.07.01 ·007/2018 se echa en falta un análisis reforzado que dé cuenta cómo es que las comunicaciones privadas configuran un dato personal y por ende, de qué forma resulta posible la aplicación de la Ley General de Datos. Ese análisis, sin embargo, no se encuentra contenido en la resolución.

Del mismo modo, no se aprecia que en el procedimiento en la materia se justifique alguna excepción por parte de la entonces PGR con el propósito de tratar los datos personales a través del software de espionaje telefónico. Adicionalmente, no se hace mención en dicho procedimiento si se facultó a la Procuraduría para intervenir comunicaciones por medio de una orden judicial o bien, los razonamientos de por qué no se requirió tal medida ante el Poder Judicial de la Federación.

Si bien la respuesta antes estos planteamientos podría ser negativa, ello robustecería la resolución recaída por parte del INAI, al tiempo que podría ampliar el ámbito de transgresiones efectuadas por parte de la Procuraduría.

Esto es así, en virtud que se advierte que derivado de la intensidad de la violación en las comunicaciones, se estima que no solo se transgredió el deber de seguridad y al principio de responsabilidad, sino que se transgredió todos los principios en la materia debido de la ilicitud de esa invasión.

Adicionalmente, por lo que hace a la denuncia presentada por parte del INAI, se estima que su alcance debió dar cuenta no solo de un ejercicio ilícito del deber público, sino además en torno a la violación de comunicaciones privadas, al ser información protegida al ser una categoría de datos personales. No obstante, la denuncia se ciñó a exclusivamente a evidenciar el presunto ejercicio ilícito del deber público y con ello, fue omiso

V. Contrastes entre la protección de comunicaciones privadas y la protección de datos: diferencias regulatorias.

Llegados hasta este punto, estimamos que existen divergencias para efectos de las comunicaciones privadas. Este trato diferenciado se evidencia jurídicamente respecto de los límites que se establecen para su protección.

De este modo, tal como se esquematiza a continuación, existe un espectro más amplio de excepción en el tratamiento de las comunicaciones privadas desde la protección de datos personales. En otras palabras, en vez de reforzar su tutela, paradójicamente, la protección de datos desprotege las conversaciones entre particulares.

El trato diferenciado radica en que desde la óptica de la inviolabilidad de comunicaciones la regla general es que en materia de comunicaciones privadas solo es justificable el que una autoridad acceda a estas a través de una orden judicial. Asimismo, únicamente el Ministerio Público de la Federación deberá justificar algún indicio que vincule a esa persona con el crimen organizado.

Por ende, advertimos que desde la perspectiva de la inviolabilidad de las comunicaciones, el Ministerio Público, a través de una orden judicial bajo determinado tiempo, deberá realizar esa intervención por tratarse de presuntos actos relacionados con el crimen organizado.

Por el contrario, el derecho a la protección de datos personales tiene un ámbito de excepción mucho más amplio. En otras palabras, se permiten más excepciones para uso por parte de la autoridad que restricciones. Se dice, así pues, como se analizó previamente, existen causas para restringir este derecho en lo relativo a seguridad nacional y pública, orden público, salud y derechos de terceros.

Máxime que, conforme a las disposiciones secundarias en la materia se desprende que existen numerosos supuestos que permiten exceptuar del consentimiento de la información para su tratamiento por parte de los sujetos obligados en el sector público.

Del mismo modo, se aprecia que las comunicaciones privadas no detentan un ámbito especial de protección expresamente reservado en las disposiciones secundarias, pese a la sensibilidad de la información que es posible obtener al captar este tipo de comunicaciones.

Tal cuestión se ilustra a través de la tabla que se inserta para tales efectos:

Excepciones para el acceso a comunicaciones privadas por parte de terceros.[7]

Inviolabilidad de comunicaciones privadas (Artículo 16 CPEUM, párrafos décimo segundo y décimo tercero)	**Protección de datos personales (Artículo 16 CPEUM, párrafo segundo)**
Debe concurrir: i. Limitadas a los Ministerios Públicos ii. Previa orden del Poder Judicial de la Federación iii. Limitada a un tiempo, sujetos y el tipo de intervención iv. Prohibición expresa sobre materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.	De forma separada: • Seguridad nacional • Disposiciones de orden público. • Seguridad pública • Salud pública • Protección de derechos de terceros.

Fuente: Elaboración propia

Con base en los elementos descritos a lo largo del presente análisis se estima que es posible arribar a las premisas siguientes a manera de conclusiones:

A través de la esquematización que resume el estudio efectuado al marco jurídico y su aplicación tratándose de comunicaciones privadas, queda claro que se comprueba la hipótesis que se ofreció en un principio: se genera una suerte de desprotección sobre las comunicaciones privadas desde la óptica del derecho a la protección de datos personales. Esta falta de tutela se genera a partir de un halo de excepciones mucho más amplio y en el cual no existe un escrutinio estricto con controles, como resulta ser la orden judicial.

De forma secundaria, se demuestra que el espionaje efectuado por parte de las autoridades en contra de las y los particulares es realizado bajo razonamientos de supuesta seguridad nacional e interés público, amparados en el marco jurídico de la protección de datos personales, el cual les permite instrumentar actividades intrusivas - e ilegales - en contra de las personas.

Por lo tanto, a partir del planteamiento formulado se obtiene que la protección de datos personales es omisa en poner énfasis en las comunicaciones privadas como un dato personal de especial relevancia.

En las comunicaciones privadas concurren – entre otros derechos – la inviolabilidad de comunicaciones y la protección de datos personales. No obstante, para efectos del sector público a luz del marco jurídico – así como del caso Pegasus y Raymundo Ramos – es posible notar que existe un trato diferenciado de estos derechos donde la protección de datos personales no garantiza efectivamente este tipo de comunicaciones.

Así, se aprecia que las comunicaciones privadas desde este último derecho, no conceden un ámbito de protección especial en virtud de las numerosas excepciones para el tratamiento de datos personales.

Por lo tanto, se comprueba la (des)protección de datos personales derivado de que los sujetos obligados como la SEDENA y FGR realizan un tratamiento ilícito de las comunicaciones privadas amparados en razonamientos de seguridad nacional e interés público.

Sobre los casos Pegasus y Raymundo Ramos, desde la óptica del derecho a la protección de datos personales se estima que las comunicaciones privadas se encuentran vulnerables. Esto es

[7] Únicamente se da cuenta de las consideraciones de excepción que se desprenden a nivel constitucional sin incorporar las consideraciones establecidas en la legislación secundaria.

así en razón que, producto del procedimiento de investigación únicamente se acreditó que la entonces PGR transgredió los principios de seguridad y el principio de responsabilidad. Nada se dice sobre la violación de comunicaciones privadas.

Adicionalmente, en ningún momento se presentó una denuncia por la ilegal intervención de comunicaciones, sino únicamente por entorpecer las actividades del INAI para el indebido ejercicio función pública.

Por lo que hace al caso de defensor de derechos humanos Raymundo Ramos, se aprecia que la intervención de comunicaciones es una práctica continua por parte de las autoridades del sector público. No solo eso, sino que hay indicios de un aparato de inteligencia militar que funciona fuera del marco jurídico.

Cabe destacar que, ante los cuestionamientos del por qué se llevan a cabo estas actividades consideradas espionaje, el Titular del Poder Ejecutivo Federal argumentó que su objetivo es realizarlo con base en actividades de inteligencia.[8]

De tal suerte, con base en las declaraciones del Presidente de la República, es claro que se realizan actividades de intervención de comunicaciones por parte de las fuerzas armadas justificados en una suerte de actividades de seguridad denominado como inteligencia.

Cuestión que deviene crucial pues no se advierte qué controles existen, ni tampoco qué facultades poseen las fuerzas armadas para intervenir comunicaciones. Tan es así que como se ha sostenido, con base en los criterios judiciales, este tipo de intervención es facultad exclusiva de los ministerios públicos a través de orden judicial.

Sin embargo, tal como se evidenció en las medidas del caso Pegasus que fue radicado en el INAI, se estima que estas fueron limitadas únicamente de forma temporal, ceñidas a una presunta desinstalación del software de espionaje.

Esto nos lleva al punto actual, que ante la falta de medidas ejemplares concatenadas con la falta del impulso de una política para acotar la intervención de comunicaciones por parte de las fuerzas armadas - las cuales comprenden a las Secretarías de Defensa, de Marina, de Gobernación y Guardia Nacional – nos encontremos de nueva cuenta en una fase de repetición en el espionaje en contra de personas que no se vinculan con la delincuencia organizada o con amenazas en contra de la seguridad nacional.

De tal suerte, se aduce que no existe una concepción reforzada de este derecho por parte de las autoridades competentes en la materia, pues el INAI planteó una controversia en el expediente que se estima restrictiva para efectos de garantizar adecuadamente este derecho.

En este orden de ideas, es evidente que se alcanzan los objetivos de la investigación, pues ligado a la verificación de la hipótesis en la que se soporta este estudio, queda claro que el marco jurídico de la protección de datos en vez de reforzar las comunicaciones privadas. En esa misma línea, se alcanza el objetivo secundario, pues queda evidenciado que las autoridades emplean esta discrecionalidad para emprender acciones de espionaje contra periodistas y activistas, amparado en el marco jurídico de la protección de datos personales.

[8] Al respecto, véase la versión estenográfica de la conferencia matutina del Presidente de la República que, en su parte conducente mencionó: *"PRESIDENTE ANDRÉS MANUEL LÓPEZ OBRADOR: Bueno, se tiene que hacer investigación, que no espionaje, que es distinto. Y el instituto de inteligencia del gobierno hace investigación, porque nosotros sostenemos que es muy importante hacer la investigación, inteligencia, para no usar la fuerza, es mejor la inteligencia que la fuerza."*https://lopezobrador.org.mx/2023/03/10/version-estenografica-de-la-conferencia-de-prensa-matutina-del-presidente-andres-manuel-lopez-obrador-927/

Asimismo, del pronunciamiento por parte del Gobierno Federal antes analizado, se estima que no existe congruencia en las manifestaciones esgrimidas por parte de la autoridad, en razón que no se da cuenta de qué clase de método se utiliza para intervenir al crimen organizado, ni tampoco se clarifica cuál es el marco normativo que faculta a las fuerzas armadas a cometer espionaje contra civiles, particularmente, para intervenir sus comunicaciones privadas.

También, como se mencionó previamente, se aluden a atribuciones en torno a la defensa del orden público mas no se invoca ninguna clase de precepto legal que faculte a esas instancias para intervenir comunicaciones. Máxime que las comunicaciones privadas son inviolables conforme a lo establecido a nivel constitucional.

De tal suerte, se aprecia el que se genera un incentivo para intervenir comunicaciones por parte de las fuerzas de orden público sin que exista rendición de cuentas, ni procedimientos robustos en contra de las autoridades que cometen esta clase de intervenciones.

Finalmente, se advierten amplios espacios de oportunidad por lo que hace a la forma en la cual el INAI ha ejercido sus atribuciones en estos casos. Se dice así, en razón que, por lo que se refiere al caso de espionaje cometido a través del software Pegasus, el cual se encuentra ampliamente documentado, ese Instituto no adoptó un enfoque sobre inviolabilidad de comunicaciones. Tampoco, reforzó el marco jurídico sobre este aspecto.

Es decir, no se sentó un precedente sobre la sensibilidad de la intervención de comunicaciones privadas. Por cuanto al espionaje cometido en contra de Raymundo Ramos, a la fecha no se tiene noticia que ese Organismo Garante se pronunciara al respecto, mucho menos que comenzara con una investigación de forma proactiva con el propósito de verificar si se había dado una transgresión en contra de la información personal del activista.

VI. A manera de conclusión: primeros trazos para un remedio jurídico y políticas para un posible reforzamiento en la intervención de comunicaciones

Recordemos que de conformidad con lo dispuesto en los artículos 16 y 17 de la Ley General de Datos, se establece que los sujetos obligados del sector público deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Así, el tratamiento de datos personales por parte de las autoridades deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

Este punto resulta fundamental, en tanto que, el principio de licitud establece el tratamiento de la información a partir de las facultades y atribuciones de los sujetos obligados; por lo tanto, es posible impulsar no solo códigos de ética sino procedimientos de verificación para los responsables del sector público.

Adicionalmente, se estima que existe una ventana de oportunidad respecto de un procedimiento ejemplar para efectos del caso Raymundo Ramos e indagar qué clase de software, las autoridades involucradas y bajo qué razonamiento fueron efectuadas estas intervenciones.

Con base en el principio pro persona contenido en el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos, resultaría posible el explorar la viabilidad de la aplicación de las disposiciones en materia de inviolabilidad de comunicaciones de forma supletoria al de protección de datos personales cuando se presenten estos casos.

En este sentido, si bien no es el objeto del presente estudio, las autoridades administrativas no pueden inaplicar normas o bien declarar la inconstitucionalidad de las mismas, lo cierto es que podría reforzarse el dictado del procedimiento de verificación a partir de la mencionada duplicidad en la naturaleza de las comunicaciones privadas con base en el principio pro persona con el propósito de ser garantista por lo que hace a este bien jurídico.

Sobre las posibles reformas en la materia. Con todo, pueden existir propuestas para reformar el marco jurídico en materia de responsabilidades administrativas, penal o civil con mayor severidad. No obstante, acotado al ámbito de las disposiciones en materia de protección de datos personales, se estima que no es necesario reformar por el momento ningún instrumento normativo en la materia.

Por el contrario, las disposiciones actuales ya ofrecen una salida que viene aparejado del uso intensivo de las facultades del INAI con el propósito de prevenir que se repita la intervención de comunicaciones. Simultáneamente, es necesario impulsar el que los procesos de verificación radicados ante ese Organismo les recaigan resoluciones que adopten una perspectiva garantista y que aborden de forma exhaustiva el fondo de la controversia planteada: es decir, la intervención de comunicaciones desde la protección de datos personales.

Bibliografía

Basterra, M. I. (2008). *Protección de datos personales*. EDIAR-UNAM.

Brizzolis, F. (2019). Pegasus: El eterno espionaje que ha sido descubierto en los últimos tiempos.

Cejudo, G. (Coord.). (2019). *Diccionario de Transparencia y Acceso a la Información Pública*. México. INAI.

Cienfuegos Salgado, (2012). Nota a propósito de la inviolabilidad de las comunicaciones privadas.

Gómez Robledo, A., & Ornelas Núñez, L. (2006). *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*. Instituto de Investigaciones Jurídicas (Ed.), Serie Estudios Jurídicos. 97. 6-19. México. UNAM.

Pascual Huerta, P. (2017). *La génesis del derecho fundamental a la protección de datos personales* (Tesis doctoral, Universidad Complutense, Madrid).

Normatividad consultada

Constitución Política de los Estados Unidos Mexicanos, artículo 16.

Convención Americana sobre Derechos Humanos.

Declaración Universal de Derechos Humanos.

Ley Federal contra la Delincuencia Organizada.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Tesis, jurisprudencia y resoluciones

Amparos directos en revisión 975/2018 y 1621/2010.

Expediente de verificación INAI.3S.07.01-007/2018.

Tesis Aislada P. VII/2014 (10a.). Pleno. Décima Época. Registro 2005879. Gaceta del Semanario Judicial de la Federación. Libro 4, marzo, 2014, 222. "AUTORIDADES ADMINISTRATIVAS. NO ESTÁN FACULTADAS PARA INAPLICAR NORMAS QUE ESTIMEN DEROGADAS POR EL ARTICULO NOVENO TRANSITORIO DEL DECRETO DE REFORMA CONSTITUCIONAL PUBLICADO EN El DIARIO OFICIAL DE LA FEDERACIÓN EL 10 DE JUNIO DE 2011.

Tesis aislada 1a. CLIII/2011 "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SUS DIFERENCIAS CON EL DERECHO A LA INTIMIDAD.

Tesis con número de registro 169700 2a. LXIII/2008: DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

Informes y notas periodísticas

Así logró el software Pegasus espiar a 25 periodistas mexicanos, Forbes México, julio 2021, visible en: https://www.forbes.com.mx/tecnologia-asi-software-pegasus-espiar-25-periodistas-mexicanos/

Acciones de inteligencia, orientadas a atender amenazas y riesgos a la seguridad nacional, Comunicado, 23 de marzo, 2023, visible en: https://www.gob.mx/presidencia/prensa/acciones-de-inteligencia-orientadas-a-atender-amenazas-y-riesgos-a-la-seguridad-nacional

Boletín INAI/054/19, INAI, 20 de febrero, 2019.

El Ejército mexicano espió con Pegasus al activista Raymundo Ramos para interferir en una investigación sobre ejecuciones extrajudiciales, El País, México, 07 de marzo, 2023, https://elpais.com/mexico/2023-03-07/el-ejercito-mexicano-espio-con-pegasus-al-activista-raymundo-ramos-para-interferir-en-una-investigacion-sobre-ejecuciones-extrajudiciales.html

Estructura secreta del Ejército espió con Pegasus a Raymundo Ramos, con pleno conocimiento del Secretario de la Defensa, Artículo 19, 7 de marzo, 2023.

Pegasus: el programa que espía a políticos y gobiernos, Periódico la Vanguardia, 09 de mayo de 2022, https://www.lavanguardia.com/vida/junior-report/20220509/8248278/pegasus-espionaje-politicos-gobiernos.html

Red de defensa de derechos digitales, Lo que sabemos de las autoridades que adquirieron Pegasus en México, julio 2023, visible en: https://r3d.mx/2021/07/23/autoridades-pegasus-mexico/

Versión estenográfica del Ejecutivo Federal de fecha 10 de marzo, 2023 visible en: https://lopezobrador.org.mx/2023/03/10/version-estenografica-de-la-conferencia-de-prensa-matutina-del-presidente-andres-manuel-lopez-obrador-927/